REMARKS

This Application has been carefully reviewed in light of the Final Office Action. Claims 1-21 are pending in the Application. The Final Office Action rejects Claims 1-21. Applicant respectfully requests reconsideration and favorable action in this case.

Section 102 Rejections

The Final Office Action rejects Claims 1-21 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 7,152,105 to McClure et al. ("*McClure*"). Applicant respectfully traverses these rejections for the reasons described below.

At the outset, Applicant provides a reminder that in order to establish a *prima facie* case of anticipation, "[t]he identical invention must be shown in as complete detail as is contained in the ... claim" (*Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)), and that the elements must be arranged as required by the claim (*In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990)). Furthermore, "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987). With these threshold requirements in mind, Applicant submits that the Final Office Action has failed to establish a *prima facie* case of anticipation using *McClure*.

Independent Claim 1 is allowable at least because *McClure* fails to disclose, expressly or inherently, "receiving, from a network intrusion detection sensor, one or more data packets associated with an alarm indicative of a potential attack on a target host; identifying characteristics of the alarm from the data packets, including at least an attack type and an operating system fingerprint of the target host; and identifying the operating system type from the operating system fingerprint." In contending that *McClure* discloses "receiving, from a network intrusion detection sensor, one or more data packets associated with an alarm indicative of a potential attack on a target host" of Claim 1, the Final Office Action states:

> McClure discloses sometimes, in order to "force" a response from the target computer, an intruder may send a malformed packet to a target port. While this known technique increases the likelihood that an open UDP port on the target computer can be identified, this technique also substantially increases the likelihood that the malformed packet could damage the target computer.

See Final Office Action, Page 2. Even if this is correct, which Applicant does not address, *McClure* fails to disclose this element arranged with every other element of Independent Claim 1, as required. In short, the passage relied on by the Final Office Action to teach this limitation refers to a different device than the device relied on by the Final Office Action to teach the other limitations of Claim 1—neither of these devices disclose the claimed method with all of the claimed limitations.

For example, the Final Office Action further relies on the passage of *McClure* at Col. 17, Line 29 - Col. 18, Line 50 to disclose "identifying characteristics of the alarm from the data packets, including at least an attack type and an operating system fingerprint of the target host; and identifying the operating system type from the operating system fingerprint" of Independent Claim 1. *See Final Office Action*, Page 3. The passage of *McClure*, however, expressly discloses identifying an operating system using RFC-compliant packets, and not malformed packets:

> The present system typically employs a unique set of new features to maximize the accuracy of operating system detection while minimizing intrusiveness and interference with operations of the target computer. In one embodiment, the invention sends RFC-compliant TCP "SYN" (synchronization) packets to a target computer. The use of RFC-compliant TCP packets advantageously reduces the probability that the detection packets are blocked by a router or firewall, and greatly reduces the probability that the detection packets will cause damage or crashes at the target computer.

See McClure, Col. 16, Lines 57-67 (emphasis added). According to the passage, the packets of *McClure* are RFC-compliant, and therefore, are clearly not the malformed packets that the Final Office Action relies upon to disclose "receiving, from a network intrusion detection sensor, one or more data packets associated with an alarm indicative of a potential attack on a target host" of Claim 1, as discussed above. Rather, the passage refers to sending malformed packets in some other device, but not the device relied on in the Office Action as anticipating the present claim:

> The intelligent UDP port scanning test in accordance with this embodiment of the present invention employs an efficient, less intrusive and more accurate method for scanning UDP ports on a target computer.

See McClure, Col. 24, Lines 22-25 (emphasis added). As a result, *McClure* fails to disclose, expressly or inherently, a computerized method that includes all of the following limitations: "receiving, from a network intrusion detection sensor, one or more data packets associated

with an alarm indicative of a potential attack on a target host; identifying characteristics of the alarm from the data packets, including at least an attack type and an operating system fingerprint of the target host; and identifying the operating system type from the operating system fingerprint" arranged as required by Claim 1.

For at least this reason, Independent Claim 1 is allowable, as are Claims 2-6 that depend therefrom. For analogous reasons, Independent Claims 7 and 16 are allowable, as are Claims 8-15 and 17-21, respectively, that depend therefrom. Reconsideration and favorable action are requested.

CONCLUSION

Applicant has made an earnest attempt to place this case in condition for allowance. For the foregoing reasons, and for other apparent reasons, Applicant respectfully requests full allowance of all pending Claims.

If the Examiner feels that a telephone conference would advance prosecution of this Application in any manner, the Examiner is invited to contact Brad P. Williams, Attorney for Applicant, at the Examiner's convenience at (214) 953-6447.

Applicant believes no fee is due. However, should there be a fee discrepancy, the Commissioner is hereby authorized to charge any required fees or credit any overpayments to Deposit Account No. **02-0384** of **Baker Botts L.L.P.**

Respectfully submitted,
BAKER BOTTS L.L.P.
Attorneys for Applicant

Bradley P. Williams
Reg. No. 40,227

Date: July 27, 2007

Correspondence Address:

Customer Number: **05073**